UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MICHAEL MUTZ, *On behalf of himself and others similarly situated,* Plaintiff, v. CENTIMARK CORPORATION, Defendant.	Case No:

DECLARATION OF COURTNEY K. MAZZIO IN SUPPORT OF DEFENDANT'S NOTICE OF REMOVAL

I, Courtney K. Mazzio, Esquire, hereby declare as follows:

1. I am an attorney at law licensed to practice in the Commonwealth of Pennsylvania and I am a member of the Bar of this Court. I am an associate with the law firm Gordon Rees Scully Mansukhani, LLP, attorneys for Defendant Centimark Corporation ("Defendant") and I am familiar with the facts of this matter.

2. Attached as Exhibit A to this Declaration is a true and accurate copy of the Complaint captioned *Michael Mutz v. Centimark Corporation,* Case No. C-48-CV-2023-1012, currently pending in the Pennsylvania Court of Common Pleas, Northampton County.

3. Attached as Exhibit B is a true and accurate copy of the civil docket in the action *Michael Mutz v. Centimark Corporation,* Case No. C-48-CV-2023-1012, currently pending in the Pennsylvania Court of Common Pleas, Northampton County.

4. Defendant received notice of the Complaint on February 22, 2023.

Pursuant to 28 U.S.C. §1746, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Respectfully submitted,

GORDON REES, SCULLY, MANSUKHANI LLP

Dated: March 23, 2023

/s/ Courtney K. Mazzio

Peter Siachos, Esquire (PA ID# 318250)
Courtney Mazzio, Esquire (PA ID#319642)
1717 Arch Street, Suite 610
Philadelphia, PA 19103
psiachos@grsm.com
cmazzio@grsm.com
Counsel for Defendant,
Centimark Corporation

EXHIBIT A

Supreme Court of Pennsylvania

Court of Common Pleas
Civil Cover Sheet

Northampton County

For Prothonotary Use Only:	
Docket No: C-48-CV-2023-	1012

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

SECTION A

Commencement of Action:
- [x] Complaint
- [ ] Writ of Summons
- [ ] Petition
- [ ] Transfer from Another Jurisdiction
- [ ] Declaration of Taking

Lead Plaintiff's Name:	Lead Defendant's Name:
MICHAEL MUTZ	CENTIMARK CORPORATION
Are money damages requested? [x] **Yes** [ ] **No**	Dollar Amount Requested: (check one) [ ] within arbitration limits [x] outside arbitration limits
Is this a *Class Action Suit*? [x] **Yes** [ ] **No**	**Is this an *MDJ Appeal*?** [ ] **Yes** [x] **No**

Name of Plaintiff/Appellant's Attorney: Patrick Howard

[ ] **Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)**

SECTION B

Nature of the Case: Place an "X" to the left of the **ONE** case category that most accurately describes your ***PRIMARY CASE.*** If you are making more than one type of claim, check the one that you consider most important.

TORT (*do not include Mass Tort*)
- [ ] Intentional
- [ ] Malicious Prosecution
- [ ] Motor Vehicle
- [ ] Nuisance
- [ ] Premises Liability
- [ ] Product Liability (*does not include mass tort*)
- [ ] Slander/Libel/ Defamation
- [ ] Other:

MASS TORT
- [ ] Asbestos
- [ ] Tobacco
- [ ] Toxic Tort - DES
- [ ] Toxic Tort - Implant
- [ ] Toxic Waste
- [ ] Other:

PROFESSIONAL LIABLITY
- [ ] Dental
- [ ] Legal
- [ ] Medical
- [ ] Other Professional:

CONTRACT (*do not include Judgments*)
- [ ] Buyer Plaintiff
- [ ] Debt Collection: Credit Card
- [ ] Debt Collection: Other
- [ ] Employment Dispute: Discrimination
- [ ] Employment Dispute: Other
- [ ] Other:

REAL PROPERTY
- [ ] Ejectment
- [ ] Eminent Domain/Condemnation
- [ ] Ground Rent
- [ ] Landlord/Tenant Dispute
- [ ] Mortgage Foreclosure: Residential
- [ ] Mortgage Foreclosure: Commercial
- [ ] Partition
- [ ] Quiet Title
- [ ] Other:

CIVIL APPEALS
Administrative Agencies
- [ ] Board of Assessment
- [ ] Board of Elections
- [ ] Dept. of Transportation
- [ ] Statutory Appeal: Other
- [ ] Zoning Board
- [ ] Other:

MISCELLANEOUS
- [ ] Common Law/Statutory Arbitration
- [ ] Declaratory Judgment
- [ ] Mandamus
- [ ] Non-Domestic Relations Restraining Order
- [ ] Quo Warranto
- [ ] Replevin
- [x] Other: Data Breach

Updated 1/1/2011

SALTZ MONGELUZZI & BENDESKY P.C.
BY: PATRICK HOWARD
IDENTIFICATION NO: 88572
1650 MARKET STREET
52ND FLOOR
PHILADELPHIA, PA 19103
(215) 496-8282

TURKE & STRAUSS LLP
BY: RAINA C. BORRELLI/SAMUEL J. STRAUSS
PRO HAC VICE PENDING
613 WILLIAMSON STREET, SUITE 201
MADISON, WI 53703
(608) 237-1775

Attorneys for Plaintiff

MICHAEL MUTZ
1501 Cottage Street
Easton, PA 18040,

On behalf of himself and others similarly situated,

Plaintiff,

v.

CENTIMARK CORPORATION
12 Grandview Circle
Canonsburg, PA 15317,

Defendant.

NORTHAMPTON COUNTY COURT OF COMMON PLEAS

No.

CLASS ACTION COMPLAINT IN A CIVIL ACTION

JURY TRIAL DEMANDED

NOTICE

"You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by an attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DO NOT HAVE A LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP.

THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER.

IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE.

NORTHAMPTON COUNTY BAR ASSOCIATION
LAWYER REFERRAL SERVICE
P.O. BOX 4733
Easton, Pennsylvania 18042
(610) 258-6333

AVISO

Le han demandado en corte. Si usted quiere defenderse contra las demandas nombradas en las páginas siguientes, tiene veinte (20) dias, a partir de recibir esta demanda y la notificatión para entablar personalmente o por un abogado una comparecencia escrita y tambien para entablar con la corte en forma escrita sus defensas y objeciones a las demandas contra usted. Sea avisado que si usted no se defiende, el caso puede continuar sin usted y la corte puede incorporar un juicio contra usted sin previo aviso para conseguir el dinero demandado en el pleito o para conseguir culquier otra demanda o alivio solicitados por el demandante. Usted puede perder dinero o propiedad u otros derechos importantes para usted.

USTED DEBE LLEVAR ESTE DOCUMENTO A SU ABOGADO INMEDIATAMENTE. SI USTED NO TIENE ABOGADO (O NO TIENE DINERO SUFICIENTE PARA PARGAR A UN ABOGADO), VAYA EN PERSONA O LLAME POR TELEFONO LA OFICINA NOMBRADA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASSISTENCIA LEGAL. ESTA OFICINA PUEDE PROPORCIONARLE LA INFORMACION SOBRE CONTRATAR A UN ABOGADO.

SI USTED NO TIENE DINERO SUFICIENTE PARA PAGAR A UN ABOGADO, ESTA OFICINA PUEDE PROPORCIONARLE INFORMACION SOBRE AGENCIAS QUE OFRECEN SERVICIOS LEGALES A PERSONAS QUE CUMPLEN LOS REQUISITOS PARA UN HONORARIO REDUCIDO O NINGUN HONORARIO.

ASSOCIACION DE LICENDIADOS DE
NORTHAMPTON
SERVICO DE REFERENCA E INFORMACION LEGAL
P.O. BOX 4733
Easton, Pennsylvania 18042
Telefono: (610) 258-6333

CLASS ACTION COMPLAINT

Plaintiff, Michael Mutz, on behalf of himself and all others similarly situated, states as follows for his class action complaint against defendant, CentiMark Corporation, ("CentiMark" or "Defendant"):

INTRODUCTION

1. In August 2022, CentiMark, a commercial roofing company headquartered in Pennsylvania, with over 95 offices throughout the United States, lost control of its computer network and the highly sensitive personal information stored on that network in a data breach by cybercriminals ("Data Breach"). The number of total breach victims is unknown, but on information and belief, the Data Breach has impacted at least thousands of former and current employees.

2. On information and belief, the Data Breach began on or around August 7, 2022, and was not discovered by CentiMark until August 11, 2022. Following an internal investigation, Defendant learned cybercriminals gained unauthorized access to current and former employees' "personally identifiable information" ("PII"), including names, dates of birth, Social Security numbers, and driver's license numbers.

3. On information and belief, cybercriminals bypassed Defendant's inadequate security systems to access employee's PII in its computer systems.

4. On or around December 2, 2022, -- nearly four months after the Data Breach first occurred – Defendant finally began notifying victims about the breach (the "Breach Notice") which is attached as **Exhibit A**.

5. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its employees how many people were impacted, how the breach happened,

or why it took the Defendant nearly four months to begin notifying victims that hackers had gained access to highly sensitive PII.

6. Defendant's failure to timely detect and report the Data Breach made its current and former employees vulnerable to identity theft without any warning that they should monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

8. In failing to adequately protect employees' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed an unknown number of its current and former employees.

9. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

10. Plaintiff Mutz is a former CentiMark employee and Data Breach victim. Mr. Mutz worked for a CentiMark affiliate in the 1990s and again from 2011 through 2016 and, as a condition of that employment, was required to provide his PII to CentiMark. Plaintiff Mutz reasonably believed that CentiMark would take adequate steps to safeguard the PII he entrusted to it. Defendant did not, resulting in the Data Breach.

11. Accordingly, Plaintiff, on his own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in

Defendant's possession.

PARTIES

12. Plaintiff, Michael Mutz, is a natural person and citizen of Pennsylvania, residing in Easton, Pennsylvania, where he intends to remain. Mr. Mutz is a former CentiMark employee and Data Breach victim, receiving CentiMark's Breach Notice in December 2022.

13. Defendant, CentiMark, is a Pennsylvania corporation with its principal place of business at 12 Grandview Circle, Canonsburg, PA 15317.

JURISDICTION & VENUE

14. This Court has subject matter jurisdiction over this action under 42 Pa. Cons. Stat. § 931.

15. This Court has personal jurisdiction over Defendant because Defendant is incorporated and headquartered in Pennsylvania and conducts a significant portion of its general business in Pennsylvania.

16. Venue is proper under 231 Pa. Code § 2179 because Defendant regularly conducts business in Northampton County.

BACKGROUND FACTS

a. CentiMark

17. On information and belief, CentiMark is a Pennsylvania corporation providing commercial roofing solutions for its customers. According to its website, CentiMark takes "great pride in the people, dedication and professionalism that drives us to new levels of success and excellence in roofing."[1] CentiMark has over 95 offices throughout the United States, Canada, and Mexico.[2]

[1] *See* CentiMark website: https://www.centimark.com/about-us/about-us-main (last visited February 9, 2023).
[2] *Id.*

18. On information and belief, CentiMark accumulates highly sensitive PII of its employees.

19. On information and belief, CentiMark maintains former employees' PII for years—even decades—after the employee-employer relationship is terminated.

20. CentiMark's Privacy Policy promises that it has, "implemented reasonable and appropriate administrative, technical, and physical safeguards to protect the security of personal information that you provide to us," and also states that, "We will comply with all applicable federal and state laws and regulations concerning the protection of the privacy and security of our customers' personal information."[3]

21. Despite recognizing its duty to do so, on information and belief, CentiMark has not implemented reasonably cybersecurity safeguards or policies to protect employee PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, CentiMark leaves vulnerabilities in its systems for cybercriminals to exploit and gain access to employee PII.

b. CentiMark Fails to Safeguard Employee PII

22. Plaintiff is a former employee of CentiMark.

23. As a condition of employment with CentiMark, Defendant requires its employees to disclose PII such as their names, Social Security numbers, and driver's license numbers.

24. On information and belief, CentiMark collects and maintains employee PII in its computer systems.

25. In collecting and maintaining the PII, CentiMark implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

[3] https://www.centimark.com/terms-conditions/privacy-policy-and-terms-of-use (last accessed Feb. 12, 2023).

26. According to the December 2, 2022, Breach Notice, CentiMark claims to have "discovered and stopped a ransomware attack" on August 11, 2022. However, its own investigation determined there was "intermittent unauthorized access to our servers between august 7, 2022 and August 11, 2022. See Exh. A.

27. Defendant's investigation revealed that its network had been hacked by cybercriminals and that Defendant's inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain files containing a treasure trove of potentially thousands of CentiMark employees' personal, private, and sensitive information, including but not limited to employees' names, date of birth, Social Security numbers, and driver's license numbers.

28. Employees place value in data privacy and security. These are important considerations when deciding who to work and provide services for. Plaintiff would not have accepted the Defendant's employment offer, nor provided their PII, to CentiMark had they known that CentiMark does not take all necessary precautions to secure the personal and financial data given to it by its employees.

29. Despite its duties and alleged commitments to safeguard PII, CentiMark does not follow industry standard practices in securing employees' PII, as evidenced by the Data Breach and stolen employee PII.

30. In response to the Data Breach, CentiMark contends that it has or will be taking the following steps: "Increasing password complexity requirements and the frequency of password changes; Adding multi-factor authentication for employee accounts; and Reviewing and strengthening our policies and procedures regarding data security." Exh. A. Although CentiMark fails to expand on these alleged "strengthening" measures, such steps should have been in place

before the Data Breach.

31. Through its Breach Notice, CentiMark also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of fraud and identity theft and fraud by regularly reviewing [their] account statements and free credit reports for any unauthorized or suspicious activity." Exh. A.

32. On information and belief, CentiMark has offered complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

33. Even with complimentary credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

34. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

35. On information and belief, CentiMark failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over employee PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that CentiMark cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly what information was stolen and when.

c. Plaintiff's Experience

36. Mr. Mutz is a former CentiMark employee who worked for CentiMark on two separate occasions, first in the 1990's and then again from 2011 through 2016.

37. As a condition of employment, CentiMark required Mr. Mutz to provide his PII.

38. Mr. Mutz provided his PII to CentiMark and trusted that the company would use reasonable measures to protect it according to CentiMark's Privacy Policy, internal policies and state law.

39. CentiMark deprived Mr. Mutz of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for nearly four months.

40. As a result of the Data Breach, Mr. Mutz has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

41. Mr. Mutz has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Mr. Mutz fears for his personal financial security and uncertainty over what PII exposed in the Data Breach. Mr. Mutz has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

42. Mr. Mutz has suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

43. Mr. Mutz has suffered imminent and impending injury arising from the

substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

44. Mr. Mutz has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

d. **Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft**

45. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

46. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, date of birth, Social Security number, or driver's license number, without permission, to commit fraud or other crimes.

47. The types of personal data compromised and potentially stolen in the CentiMark Data Breach is highly valuable to identity thieves. The employees' stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

48. Identity thieves can also use this data to harm Plaintiff and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining

> credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

49. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII in their possession.

50. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[4]

51. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

52. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

53. One such example of criminals using PII for profit is the development of "Fullz" packages.

54. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.[5]

55. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and

---

[4] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited February 12, 2023).

[5] *Id.*

sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

56. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PII.

57. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and members of the proposed Class to unscrupulous operators, con artists, and criminals.

58. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

e. Defendant failed to adhere to FTC guidelines.

59. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous

guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

60. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

61. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

62. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

64. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

f. Defendant's Offer of Credit Monitoring is Inadequate

65. At present, CentiMark has offered one or two years (depending on state of residence) of free credit monitoring provided by Experian to breach victims.

66. As previously alleged, Plaintiff's and the Class Members' personal data may exist on the Dark Web and in the public domain for months, or even years, before it is used for ill gains and actions. With only one or two years of monitoring, Plaintiff and Class Members remain unprotected from the real and long-term threats against their personal, sensitive, and private data.

67. Therefore, the "monitoring" services offered by CentiMark are inadequate, and Plaintiff and Class Members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

CLASS ACTION ALLEGATIONS

68. Plaintiff brings this action under Pa. R. Civ. P. 1701.

69. Plaintiff sues on behalf of himself and the proposed Class ("Class"), defined as follows:

> All citizens of the Commonwealth of Pennsylvania who are current and former employees of Defendant and whose PII was accessed without authorization in the Data Breach.

70. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

71. Plaintiff reserves the right to amend the class definition.

72. This action satisfies the numerosity, commonality, typicality, and adequacy requirements for suing as representative parties:

a. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of potentially thousands of members, far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class members' interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Class injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

73. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

74. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

75. Plaintiff and members of the Class entrusted their PII to CentiMark. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their personal data and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the personal data of Plaintiff's and the Class was adequately secured and protected, including using encryption technologies. Defendant further had

a duty to implement processes that would detect a breach of its security system in a timely manner.

76. CentiMark was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class's sensitive data on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

77. Defendant knew that the personal data of Plaintiff and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the personal data of Plaintiff and the Class was wrongfully disclosed, that disclosure was not fixed.

78. By being entrusted by Plaintiff and the Class to safeguard their personal data, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their personal data with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

79. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' personal data by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiff's and the other Class member's personal data.

80. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff

and the Class, their personal data would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the personal data of Plaintiff and the Class and all resulting damages.

81. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' personal data. Defendant knew its systems and technologies for processing and securing the personal data of Plaintiff and the Class had numerous security vulnerabilities.

82. As a result of this misconduct by Defendant, the personal data of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their personal data was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their personal data in that it is now easily available to hackers on the Dark Web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

83. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

84. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

85. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

86. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII;

87. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

88. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

89. Enter an award of attorneys' fees and costs, as allowed by law;

90. Enter an award of prejudgment and post-judgment interest, as provided by law;

91. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

92. Grant such other or further relief as may be appropriate under the circumstances.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class)

93. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

94. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

95. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customer information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of

Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

96. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect the PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

97. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

98. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

99. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

100. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

101. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

102. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff

and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

103. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

104. Defendant's misconduct also violated Pennsylvania's data breach notification law.

105. Defendant is a business entity that maintains, stores, or manages computerized data that includes "personal information" as defined as 73 Pa. Stat. § 2302.

106. Plaintiff's and members of the Class's PII includes "personal information" as defined by 73 Pa. Stat. § 2302.

107. Defendant was aware of a breach of its computer system that it believed or reasonably should have believed had caused or would cause loss or injury to residents of Pennsylvania.

108. Defendant had an obligation to disclose the Data Breach to Plaintiff and members of the Class in a timely fashion as mandated by 73 Pa. Stat. § 2303.

109. Defendant's failure to disclose the Data Breach in a timely manner as required by 73 Pa. Stat. § 2303 constitutes negligence per se.

110. As a direct and proximate cause of Defendant's negligence in failing to comply with 73 Pa. Stat. § 2303, Plaintiff and members of the Class sustained actual losses and damages as described herein.

111. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to

exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

112. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their personal data, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as CentiMark fails to undertake appropriate and adequate measures to protect their personal data in its continued possession.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

113. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

114. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

115. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

116. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII and PHI;

117. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

118. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

119. Enter an award of attorneys' fees and costs, as allowed by law;

120. Enter an award of prejudgment and post-judgment interest, as provided by law;

121. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

122. Grant such other or further relief as may be appropriate under the circumstances.

COUNT III
Breach of Confidence
(On Behalf of Plaintiff and the Class)

123. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

124. At all times during Plaintiff and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' personal data that Plaintiff and Class Members provided to Defendant.

125. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' personal data would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

126. Plaintiff and Class Members provided their respective personal data to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the personal data to be disseminated to any unauthorized parties.

127. Plaintiff and Class Members also provided their respective personal data to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that personal data from unauthorized disclosure, such as following basic principles of information security practices.

128. Defendant voluntarily received in confidence Plaintiff's and Class Members' personal data with the understanding that the personal data would not be disclosed or disseminated to the public or any unauthorized third parties.

129. Due to Defendant's failure to prevent, detect, and/or avoid the data breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' personal data, Plaintiff's and Class Members' personal data was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

130. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

131. But for Defendant's disclosure of Plaintiff's and Class Members' personal data in violation of the parties' understanding of confidence, their personal data would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data breach was the direct and legal cause of the theft of Plaintiff's and Class Members' personal data, as well as the resulting damages.

132. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' personal data. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class Members' personal data had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices.

133. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the data

breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

134. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

135. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

136. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

137. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

138. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII and PHI;

139. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

140. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

141. Enter an award of attorneys' fees and costs, as allowed by law;

142. Enter an award of prejudgment and post-judgment interest, as provided by law;

143. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

144. Grant such other or further relief as may be appropriate under the circumstances.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

145. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

146. Plaintiff and the Class entrusted their PII to Defendant at the time they entered into an employment relationship with Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed, based on its representations and actions, including its Privacy Policy, to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

147. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

148. Defendant breached the implied contracts they made with Plaintiff and the Class by failing to adequately safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data

Breach.

149. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

150. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

151. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

152. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

153. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

154. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII and PHI;

155. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

156. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

157. Enter an award of attorneys' fees and costs, as allowed by law;

158. Enter an award of prejudgment and post-judgment interest, as provided by law;

159. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

160. Grant such other or further relief as may be appropriate under the circumstances.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

161. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

162. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

163. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. They also conferred a benefit on Defendant by providing their employment services.

164. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII and by retaining the benefit of Plaintiff's and the Class's labor.

165. Instead of providing a reasonable level of security that would have prevented the

possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

171. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

172. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

173. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

174. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

175. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

176. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII;

177. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

178. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

179. Enter an award of attorneys' fees and costs, as allowed by law;

180. Enter an award of prejudgment and post-judgment interest, as provided by law;

181. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

182. Grant such other or further relief as may be appropriate under the circumstances.

COUNT VI
Publicity Given to Private Life
(On Behalf of Plaintiff and the Class)

183. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

184. One who gives publicity to matters concerning the private life of another, of a kind highly offensive to a reasonable man, is subject to liability to the other for invasion of his privacy.

185. As a condition of their employment, Plaintiff and the Class provided Defendant with sensitive personal information, including names, dates of birth, Social Security numbers, and driver's license numbers.

186. Defendant failed to employee adequate and reasonable security measures to prevent public disclosure of Plaintiff and the Class's private information.

187. Defendant failed to timely and reasonably notify Plaintiff and the Class about the data breach for a period of months, which made Plaintiff and the Class vulnerable to identify theft.

188. As a result of the disclosure of Plaintiff's and the Class's private information, Plaintiff has suffered a de facto injury, which entitles them to general damages.

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

189. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as the Class representative, and appoint the undersigned as Class counsel;

190. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

191. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

192. Enter an Order enjoining Defendant from further deceptive and unfair practices and making untrue statements with respect to the Data Breach and the stolen PII;

193. Enter an award in favor of Plaintiff and the Class that includes compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

194. Award restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

195. Enter an award of attorneys' fees and costs, as allowed by law;

196. Enter an award of prejudgment and post-judgment interest, as provided by law;

197. Grant Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

198. Grant such other or further relief as may be appropriate under the circumstances.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 15th day of February, 2023.

SALTZ MONGLUZZI & BENDESKY, P.C.

By: _____

Patrick Howard; ID No. 88572
1650 Market Street, 52nd Floor
Philadelphia, PA 19103
Tel: (215) 496-8282
phoward@smbb.com

Samuel J. Strauss*
Raina Borrelli*
TURKE & STRAUSS, LLP
613 Williamson Street #201
Madison, WI 53703
Tel: (608) 237-1775
Sam@turkestrauss.com
Raina@turkestrauss.com

Attorneys for Plaintiff

**Pro hac vice* motions to be filed

EXHIBIT A

CENTIMARK

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

December 2, 2022

i6797-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 SSN_DL ONLY
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF DATA SECURITY INCIDENT

Dear Sample A. Sample:

We are writing to tell you about a recent incident that may have involved unauthorized access to your personal information. CentiMark is a commercial roofing company headquartered in Canonsburg, Pennsylvania. We take this matter very seriously because we are committed to the privacy and security of all information in our possession. In an abundance of caution, we are providing this notice to inform you of the incident, offer complimentary identity monitoring services, and suggest ways that you can help protect your information, should you feel it necessary to do so.

What Happened

On August 11, 2022, CentiMark discovered and stopped a ransomware attack, in which an unauthorized third party accessed some of CentiMark's computer network. We immediately launched an investigation to determine the nature and scope of the unauthorized activity with the assistance of a nationally recognized digital forensics firm. Our investigation determined that there was intermittent unauthorized access to our servers between August 7, 2022 and August 11, 2022. Through the investigation, we learned that we would be unable to determine what specific information the unauthorized third party viewed within or acquired from our network. While we were unable to say definitively if your information was accessed or acquired by the unauthorized third party, we are notifying you of the incident in an abundance of caution.

What Information Was Involved

We found no evidence that personal information has been misused; however, it is possible that the following information about you could have been accessed by an unauthorized third party: first and last name, date of birth, Social Security number, and/or driver's license number.

What We Are Doing About It

As soon as we discovered the unauthorized activity, we worked quickly to secure our network and to investigate this incident. Our investigators also searched Dark Web sources and found no indication that any of our data had been released or offered for sale as a result of this incident. To further enhance our security and help prevent similar occurrences in the future, we have taken, or will be taking, the following steps:

1. Increasing password complexity requirements and the frequency of password changes;
2. Adding multi-factor authentication for employee accounts; and
3. Reviewing and strengthening our policies and procedures regarding data security.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate state regulators.

What You Can Do

At this time, we are not aware of any misuse of your information. However, we recommend that you take the following preventative measures to help detect and mitigate any misuse of your information.

1. Enroll in a complimentary, [Extra1]-month membership with Experian. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE; and up to $1 million in identity theft insurance. Instructions on how to activate your membership are included at the end of this letter.

2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and free credit reports for any unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.

3. Report any incidents of suspected identity theft to your local law enforcement, state Attorney General and the major credit bureaus.

For More Information

The privacy and security of your information is important to us, and we remain committed to protecting it. If you have any questions or concerns about this incident, you may call us toll-free at (888) 274-8110, Monday through Friday 9 AM – 11 PM EST, and Saturday and Sunday 11 AM – 8 PM EST. Be prepared to provide your engagement number: **ENGAGE#**.

Sincerely,

Greg Wilson
Chief Information Officer

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit https://www.experian.com/blogs/ask-experian/category/fraud-and-identity-theft/ for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to all three of the credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or

bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing ad

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

STATE SPECIFIC INFORMATION

MARYLAND residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Toll-free: 1-888-743-0023

NEW MEXICO residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State
Division of Consumer Protection
1-800-697-1220
http://www.dos.ny.gov/consumerprotection

New York Attorney General
1-800-771-7755
http://www.ag.ny.gov/home.html

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
Toll-free: 1-877-566-7226

RHODE ISLAND residents: There were 3 Rhode Island residents impacted by this incident. You have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
Toll-free: 1-401-274-4400

VERMONT residents: You may obtain information about fighting identity theft, placing a security freeze and obtaining a free copy of your credit report from the Vermont Attorney General's Office website. If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, you may call the Vermont Attorney General's Office.

Office of the Attorney General
109 State St.
Montpelier, VT 05609
http://ago.vermont.gov/
Toll-free (VT only): 1-800-649-2424
1-802-828-3171

ADDITIONAL DETAILS REGARDING YOUR [Extra1]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by**: **March 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(888) 274-8110** by **March 31, 2023**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian. A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(888) 274-8110**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for [Extra1] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.
** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

EXHIBIT B

CountySuite™ CIVIL COURT

CASE DETAILS

MICHAEL MUTZ vs. CENTIMARK CORPORATION

Public Web User Home Help

C-48-CV-2023-01012

Close

Date filed: 02/16/2023 12:12 PM

Days Open: 35

Date closed:

Status: OPEN

CIVIL: MISCELLANEOUS - OTHER

Plaintiff

Name: MICHAEL MUTZ
Address: 1501 COTTAGE STREET
EASTON, PA 18040
HOME

vs.

Defendant

Name: CENTIMARK CORPORATION
Address: 12 GRANDVIEW CIRCLE
CANONSBURG, PA 15317
BUSINESS

Attorney (Plaintiff)

Name: PATRICK HOWARD, ESQ
Address: 1650 MARKET STREET
52ND FLOOR
PHILADELPHIA, PA 19103
215-496-8282
ATTORNEY ADDRESS

Attorney

Name:
Address:

Case Details

SubCategory:

Commencement: Complaint

Filing Options: ☐ Pro Se ☑ Class Action Suit ☑ Money Damages ☑ Outside Arbitration Limits ☐ MDJ Appeal ☐ In Forma Pauperis

Disposition: Final: AOPC:

Public Notes:

Reference Nos.

Linked Cases

Case Number	Case Participants	Case Category	Opened	Status	...

Case Docket Entries

Date	Category	Description	...
3/9/2023	ENTRY OF APPEARANCE	PRAECIPE FOR ENTRY OF APPEARANCE WITH CERTIFICATE OF S...	
3/6/2023	RETURN OF SERVICE SUBMITTED	Sheriff's Return - Civil Action - Domestic - Complaint...	
2/16/2023	SERVICE-EXIT TO SHERIFF	EXIT TO SHERIFF COMPLAINT IN CIVIL ACTION ON 2/16/2023.	
2/16/2023	COMPLAINT	COMPLAINT IN CIVIL ACTION FILED BY PATRICK HOWARD, ESQ...	
2/16/2023	CASE CAPTION	CASE CAPTION IS MICHAEL MUTZ VS CENTIMARK CORPORATION ...	

Case Judgments

Date	Creditor	Debtor	Description	Amount	...